

Title (en)  
SYSTEM FOR GENERATING A SHARED CRYPTOGRAPHIC KEY AND A COMMUNICATION SYSTEM USING THE SHARED CRYPTOGRAPHIC KEY.

Title (de)  
SYSTEM ZUR ERZEUGUNG EINES GEMEINSAMEN GEHEIMÜBERTRAGUNGSSCHLÜSSELS UND KOMMUNIKATIONSSYSTEM UNTER VERWENDUNG DES GEMEINSAMEN GEHEIMÜBERTRAGUNGSSCHLÜSSELS.

Title (fr)  
SYSTEME DE GENERATION D'UNE CLE CRYPTOGRAPHIQUE PARTAGEE ET SYSTEME DE COMMUNICATIONS UTILISANT LA CLE CRYPTOGRAPHIQUE PARTAGEE.

Publication  
**EP 0277247 A1 19880810 (EN)**

Application  
**EP 87904964 A 19870731**

Priority  
• JP 8700572 W 19870731  
• JP 17865286 A 19860731  
• JP 25189686 A 19861024

Abstract (en)  
The key predistribution system generates a cryptographic key (k) shared by entities (A,B) that establish communications. A centre algorithm (G) which the centre only knows is formed under the conditions determined among a number of entities that establish communications under the control of the centre and discriminators (YA,YB) of the entities (A,B) are adapted to the centre algorithm to form secret algorithms (XA,XB) specific to each of the entities. Then the secret algorithms are loaded onto cipher forming means (2,3) such as IC cards. The cipher formes (2,3) are mounted on the individual entities (A,B) and the discriminators (YB,YA) of the other entities are applied to each other to calculate the cryptographic key (k), thereby forming the shared cryptographic key.

Abstract (fr)  
Un système de génération d'une clé cryptographique (k) partagée par des entités (A, B) qui établissent des communications est appelé en particulier système de distribution préalable de clés. Un algorithme central (G) connu uniquement d'un centre se forme dans des conditions concertées par une pluralité d'entités qui établissent des communications sous la commande du centre. Des discriminateurs (yA, yB) des entités (A, B) sont adaptés à l'algorithme central afin de former des algorithmes secrets (XA, XB) spécifiques à chaque entité. Les algorithmes secrets sont alors chargés sur un dispositif chiffreur (2, 3), tels que des cartes à circuits intégrés. Les dispositifs chiffreurs (2, 3) sont montés sur les entités individuelles (A, B) et les discriminateurs (yA, yB) des entités s'appliquent les uns sur les autres afin de calculer la clé cryptographique (k), en formant ainsi la clé cryptographique partagée. L'invention concerne en outre un système de télécommunications qui utilise ladite clé cryptographique partagée.

IPC 1-7  
**H04L 9/02**

IPC 8 full level  
**H04L 9/08** (2006.01)

CPC (source: EP US)  
**H04L 9/083** (2013.01 - EP US); **H04L 9/0847** (2013.01 - EP US)

Cited by  
USRE36310E; GB2216754A; US5311595A; GB2285562A; US5623548A; GB2285562B; GB2270446A; GB2270446B; EP0528730A1; FR2680589A1; US5301233A

Designated contracting state (EPC)  
DE FR GB IT NL

DOCDB simple family (publication)  
**EP 0277247 A1 19880810; EP 0277247 A4 19900410; EP 0277247 B1 19940504**; DE 3789769 D1 19940609; DE 3789769 T2 19940811; HK 96996 A 19960614; US 5016276 A 19910514; WO 8801120 A1 19880211

DOCDB simple family (application)  
**EP 87904964 A 19870731**; DE 3789769 T 19870731; HK 96996 A 19960606; JP 8700572 W 19870731; US 51831790 A 19900507